Marsh

提升网络复原力：强化网络安全的12项主要控制措施

2022年3月

目录

提升网络复原力：强化网络安全的12项主要控制措施

2021年，勒索软件攻击事件激增148%[1]，受此影响，网络攻击持续占据新闻报道头条位置。攻击者索要的赎金高达数百万美元；被勒索企业在支付赎金前，其运营可能受到破坏，并陷入停滞。

随着网络攻击的增加，相关的保险索赔也随之而来，这意味着承保人已经能够确定某些控制措施与相应网络事件之间的关联性。通过这种分析以及对相关数据点的持续检查，保险行业已积累起丰富的经验，深刻了解企业可以采取哪些技术措施来构建网络复原能力。

然而，随着微小损失的增多，保险公司的态度变得愈发谨慎。保险公司正在收紧承保条件，认真分析所有网络风险投保情况，并针对投保人的网络运行环境和风险控制措施提出更多质疑。

现在，企业的潜在可保性岌岌可危，采取某些控制措施已成为保险公司的最低要求。与以往相比，企业无疑更加重视控制措施，以缓释其面临的勒索软件风险，并提高其整体网络安全性和复原力。

虽然这些控制措施的最佳实践已经确立多年，但一些企业仍然止步不前，常见原因包括他们无法判断实施成本，没有进行全面部署，或者认为自己没有需求。在许多受到监管的行业（被要求采取网络复原和风险控制措施已经多年），其所做的更多是打勾选择，而不是切实提升网络安全性。

我们建议企业采取多种网络卫生措施，这对于提高企业的网络复原力和风险可保性至关重要。在本文中，达信介绍了12项网络安全控制措施及其特点和要求。

1. SonicWall: ‘The year of ransomware’ continues with unprecedented late-summer summer surge

1

远程访问多重身份验证以及特权或管理员用户访问

这是一项怎样的控制措施？

多重身份验证（MFA）是一个附加的登录安全层，旨在对请求访问计算机的用户进行身份验证。多重身份验证要求用户提供两条或多条下列类型的证明，包括："您知晓的东西"（例如密码/PIN）、"您拥有的东西"（例如密码识别设备或令牌）或者"您的特征"（例如生物特征）。

企业为什么应采取此项控制措施？

达信在《2021年网络风险保险理赔的演变》中发布的调查结果显示，80%的网络事件都是恶意的，通常是从破坏用户凭据开始。多重身份验证作为一种强有力的身份访问管理（IAM）手段，可阻止用户在未经授权的情况下远程访问计算机系统。

所有可远程访问的系统、应用程序和账户、所有特权和管理员用户的访问以及所有对关键或敏感数据的访问均应启用多重身份验证。

在许多情况下，精确实施多重身份验证有助于防止网络事件，例如代价高昂的勒索软件攻击。保险公司正要求企业提高网络复原力，多重身份验证将成为一个关键的起点。最终，这将提升企业的网络安全性，帮助其获得更好的网络风险保障。

企业至少应在以下方面实施多重身份验证：

- 关键资产
- 特权用户
- 远程应用程序

企业该如何实施此项控制措施？

实施此项控制措施时，我们建议企业：

1. 要求使用安全软件对所有远程登录到公司网络的用户进行多重身份验证，例如虚拟专用网络（VPN）和远程桌面协议（RDP）。
2. 无论用户位于哪里，针对所有管理员用户访问实施多重身份验证和加密。
3. 无论用户位于哪里，针对所有关键或敏感数据访问实施多重身份验证。
4. 强制使用长度超过14个字符的复杂密码，其中必须包含大小写字母、数字和符号。

为满足和执行上述要求，我们建议企业：

- 识别：
  - 可远程访问的所有系统和应用程序。
  - 关键和敏感数据，以及用于存储关键和敏感数据的所有系统和应用程序。
  - 所有高权限和管理员用户。
- 实施基于风险的身份验证，该方法根据访问特定系统会导致其受损的可能性，使用严格程度有别的认证流程。
- 将VPN及其它远程解决方案与多重身份验证结合起来使用。
- 甄别所有公司设备，尤其是那些可接受生物特征识别的设备（例如笔记本电脑和手机），作为强化身份验证的潜在工具。
- 查阅当地数据保护、隐私和生物特征数据相关法规。法规可能对使用私人设备或生物特征数据进行身份验证具有限制。
- 对所有设备启用身份验证，以避免一种设备受到破坏殃及所有。
- 实施多重身份验证前，为员工提供培训并告知其增加安全层的好处，以减少阻力和消除误会。

如需更多指导，请参阅 NIST 800-63 .


2021年，勒索软件攻击事件激增
148%。[1]

电子邮件过滤与网络安全

这是一项怎样的控制措施？

电子邮件过滤软件用于扫描收发的电子邮件，以阻止不想接收的内容。这可以减少垃圾邮件（例如推销或募捐的邮件或具有严重网络风险的钓鱼邮件）对收件人的影响。

此类被检测到的电子邮件将被自动过滤掉，因而潜在的恶意内容或者用户不想接收的内容根本不会送达用户，即使送达也会被标记出来，以便用户保持警惕。通过电子邮件安全软件，可疑和潜在恶意的电子邮件附件在安全的“沙箱”环境中受到额外检测。

网络内容过滤可以通过使用硬件或软件解决方案或者对用户访问违禁网站进行跟踪和监管来实现。用户访问的内容必须合法合规，例如赌博网站上的内容往往是这样，可疑的恶意内容也将受到过滤。同时，域名系统（DNS）过滤是一种特殊类型的内容筛选，使用DNS网络层并根据IP地址管理网站访问，从而对网络使用实施过滤并降低恶意软件风险。

企业为什么应采取此项控制措施？

恶意链接和文档是将恶意软件嵌入企业系统或窃取用户密码并最终访问关键系统的一种主要方式。网络和电子邮件过滤被视为抵御电子邮件或网络浏览相关网络攻击的“第一道防线”，即使如此，用户也可能沦为网络钓鱼攻击的受害者或者误入包含恶意内容的网站。

电子邮件过滤必不可少，因为电子邮件钓鱼作为初始攻击媒介，可能引发重大网络事件，尤其是勒索软件攻击。网络犯罪分子经常利用网络钓鱼活动窃取受害者的用户名和密码，然后访问受害者的IT系统。通过使用电子邮件安全和网络过滤技术，大量潜在的严重网络攻击从一开始就能被阻止。

至少，企业应对电子邮件中潜在的恶意附件和链接进行预筛，并使用相关工具监控网络内容，以阻止恶意访问网站的行为。

保险公司还对投保人提出了严苛的网络复原要求，以评估其可保性。电子邮件安全和网络过滤技术的实施，有助于改善承保人对企业的网络风险印象。这些控制措施是获得网络风险承保资格的关键要素，据保险公司预计，如果企业采取了这些措施，重大网络事件的数量将会减少。

企业该如何实施此项控制措施？

企业可以采取下列与恶意软件防护、电子邮件安全和网络过滤相关的安全控制措施：

- 使用技术扫描和过滤接收电子邮件中的恶意附件和链接。
- 防止在默认情况下运行启用宏的文件。
- 运用沙箱环境评估电子邮件附件，以确定其是否为恶意文件。
- 使用技术监控网络内容并阻止用户访问恶意网站或网页内容。

3

备份安全、加密和测试

这是一项怎样的控制措施？

安全、有效且准确的备份对于确保企业复原力至关重要。企业应对备份提供保护，最好是将它们与网络隔离开，或者采取多重访问控制和加密措施。定期检测对于确保数据的完整性和可用性也十分重要。

企业为什么应采取此项控制措施？

随着企业逐步转向云备份解决方案，攻击者会通过寻找管理员凭据获取访问权限，将备份删除或加密。缺乏可用备份，受害企业将别无选择，他们为恢复系统和数据而被迫支付赎金的可能性将大大增加。

定期测试备份至关重要。当您需要恢复系统时，如果备份不可用或不完整，它们就毫无意义可言。定期的测试还可以帮助IT和业务恢复团队了解恢复过程的复杂性，并识别外部合作伙伴。这通常不像轻触开关那么简单。

合适的备份能够帮助企业更迅速、更高效地从网络攻击中恢复过来。当企业遭遇勒索软件攻击时，拥有备份能够减少攻击者对受害者的影响并降低赎金勒索风险。

当系统被恶意加密时，企业通常就无法运行，因而面临着重大营业中断损失。安全备份可以缩短恢复时间，与跟攻击者谈判获取解密密钥相比，效率更高。通过测试，备份过程中的错误或故障将得到识别和快速纠正，备份数据的可靠性将大大提高。

企业该如何实施此项控制措施？

企业应审查其关键系统和资产，确保备份流程充分，并定期测试备份。企业还应将一份备份副本脱机存储，并与网络断开连接。

企业应制定灾难恢复、业务连续性和事故响应计划，以准确记录使用备份恢复系统的过程。

备份解决方案多种多样，孰优孰劣，很难评判。为真正关键的系统、数据和资产提供解决方案，是个不错的开始。


在网络安全方面，
人往往是最薄弱的环节。

4

特权用户访问管理

这是一项怎样的控制措施？

特权用户访问管理（PAM）是一种安全技术，提供更高或“特权”级别的访问权限以保护账户、凭据和操作。特权用户访问不同于“常规”访问，它承担着安全维护、系统/应用程序配置更改以及通过超级用户访问绕过安全控制等功能。

企业为什么应采取此项控制措施？

在网络安全方面，人往往是最薄弱的环节，给企业带来网络攻击风险。特权用户访问管理工具可以控制内部或机器对机器通信中机器（系统或应用程序）的特权访问，包括系统和应用程序管理配置人员。它基于“最低权限”的原则运行，这意味着用户只需最低访问权限即可履行工作职责。常见的特权用户访问管理解决方案，会监控管理员用户的会话，当发现异常会话时会生成警报。异常情况包括某一用户试图访问其职责范围或运营窗口之外的区域。

企业该如何实施此项控制措施？

首先，企业应确定特权用户访问管理行动和步骤。例如，企业可以采取基于风险的方法，识别风险最高的关键资产，然后只实施针对这些资产的解决方案。

实施特权用户访问管理行动之后，为了消除对解决方案的误解，企业应向员工说明该解决方案的构成要素、目的以及将其纳入整体网络安全组合的原因。企业还应构建PAM治理和监督计划，以防PAM绩效随着时间推移而衰减。这应包括：设定供应商和产品的遴选和绩效标准，以及开展实施后绩效评估。

在扩展使用PAM方面，企业可以将其它需要此项控制措施的资产纳入业务增长路线图中，并获得相关实施许可。

5

端点检测与响应

这是一项怎样的控制措施？

端点检测与响应（EDR）是一种针对端点的风险检测与响应机制。端点是指与内网或外部进行通信的远程设备，例如台式机、笔记本电脑、手机、服务器或物联网等。

端点是几乎任何恶意软件发动网络攻击的切入点，端点监控对于检测和阻止网络攻击至关重要，可以在网络攻击蔓延到更广泛的内部网络之前进行处置。端点检测与响应解决方案持续监控端点，从设备收集数据，并根据既定规则提供响应。

企业为什么应采取此项控制措施？

根据波耐蒙研究所（Ponemon Institute）于2020年发布的一项研究报告[2]显示，有68%的企业已经遭遇一次或多次端点攻击，企业的数据和/或IT设施因此受到破坏。该报告还指出，有68%的IT专业人士发现，端点攻击的发生频率自去年以来有所增加。端点监控至关重要，可在网络攻击扩散到更广泛的内部网络之前检测并阻止攻击。

另外，端点监控与响应控制措施会监视和记录这些端点上的活动。相关数据经过分析之后可用于检测持续性风险或“零日”漏洞（即，尚未修复的漏洞）。如果检测到安全风险，则可以检查日志记录，以确定风险的开始时间、破坏范围以及根本原因。

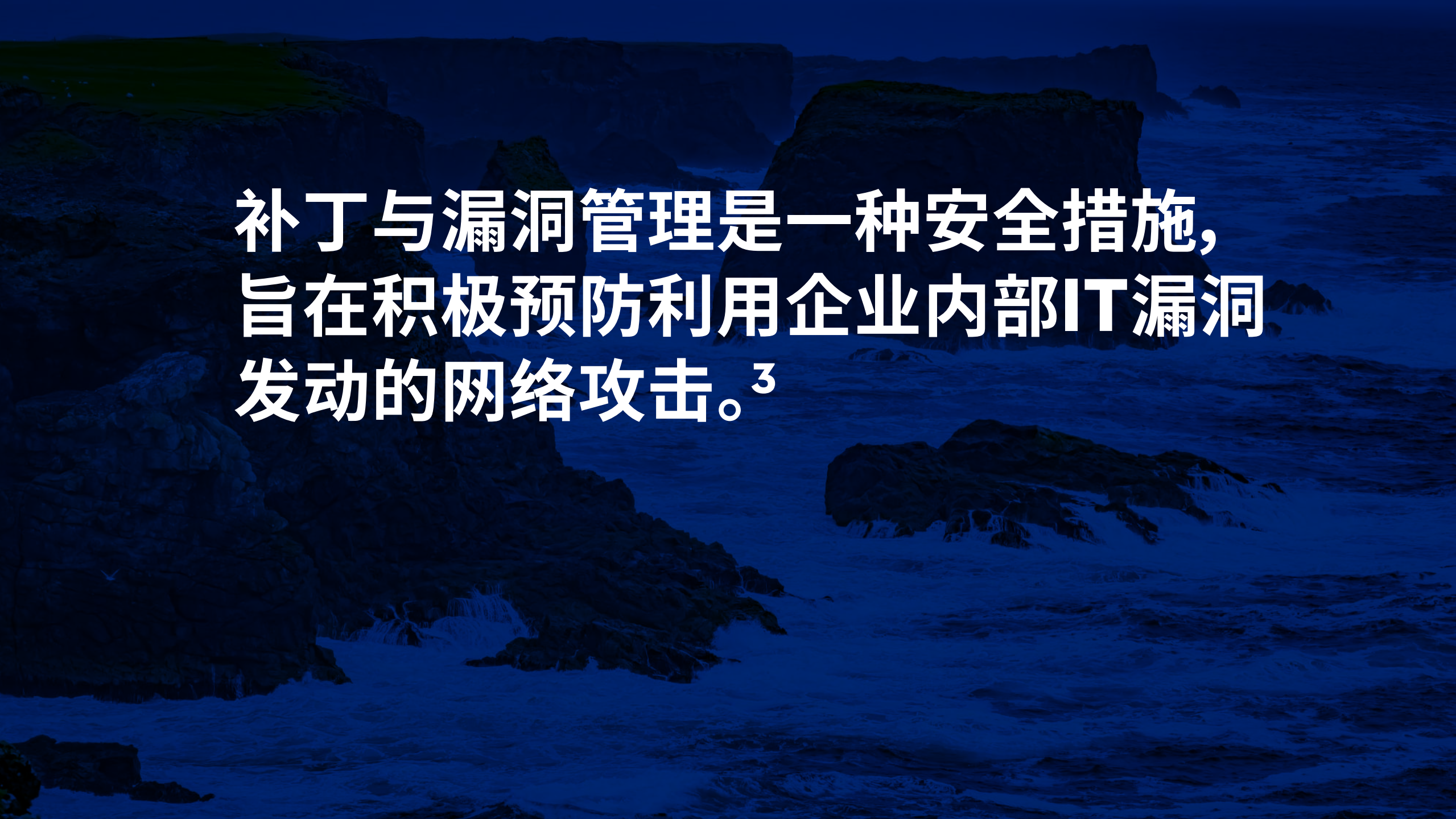
举例来说，一家企业如果没有采取端点检测与响应控制措施，则该企业在遭受勒索软件攻击之后需要更长时间才能恢复。这是因为它无法了解事件的严重程度以及有多少端点受到波及，也无法检测到是否存在任何有效负载仍在后端运行以及相关配置是否按照预期运行或需要部署的情况。所有这些都意味着恢复工作需要更长时间和更多努力。

2. 2020 State of Endpoint Security Final (morphisec.com.

企业该如何实施此项控制措施？

拥有坚实的网络安全最佳实践基础通常有助于企业无缝实施端点检测与响应控制措施。找到端点检测与响应解决方案也很重要，以最少的努力和投入换取最高级别的保护，最终无需耗费太多资源即可为贵公司的安全团队带来增值。对于一份解决方案，贵公司应重点关注以下方面：

- 贵公司所有端点的可视性：提供实时端点可视性，以便您能够查看可疑活动（即使它们只是在试图破坏您的环境），并立即阻止它们。
- 从端点收集大量遥测数据，以便通过分析技术发现攻击迹象。
- 有效的终点检测与响应需要行动方法，用于搜索攻击指标（IOAs），以便对可疑活动保持警惕，防止攻击发生。
- 纳入风险情报，包括攻击者的详细信息以及其它攻击信息。
- 实时运行，快速响应，提供准确预警，并自动应对威胁。要做到这一点，检测引擎应具有较低的误报几率，且能够设置自动响应策略。
- 拥有基于云的端点检测与响应解决方案是确保端点不受影响的唯一方法。这一解决方案应与当前的系统融合并提供直观的远程访问控制。



补丁与漏洞管理是一种安全措施，旨在积极预防利用企业内部IT漏洞发动的网络攻击。[3]

6 补丁与漏洞管理

这是一项怎样的控制措施？

漏洞管理旨在识别软硬件存在的漏洞。攻击者可能利用这些漏洞破坏设备并将其作为平台进一步实施网络攻击。

补丁管理包括软件代码修订运行系统和应用程序的通知、识别、部署、安装和验证。这些修订被称为补丁、热修复和服务包。

并非所有漏洞都有相关补丁。因此，适当的漏洞管理流程将考虑纳入其他补救措施或临时解决办法，例如软件配置变更和员工培训，以控制或规避风险。

企业为什么应采取此项控制措施？

IT漏洞总会给企业带来一定的风险。风险可以定义为系统漏洞被利用导致特定安全威胁的概率。[3]

企业常用软件和硬件设备中存在的漏洞可能被利用，由此产生多种网络安全风险。因此，如果企业没有对现有漏洞进行清晰持续的审查，将很难及时识别与应对相关风险。

另一方面，每家企业都有特定的风险承受能力，具体取决于财务状况、名誉风险及合规要求。由于管理层可能不完全了解哪些漏洞的风险最高，因此实现IT漏洞管理与风险承受能力相匹配，是个复杂的问题，且很难说服董事会。

适当的补丁与漏洞管理有助于减少或消除漏洞被利用的风险，与网络攻击发生后进行应对相比，其所需的时间、精力和金钱将大大减少。

未修补漏洞仍然是导致系统被入侵的主要原因。每个月都有数百个应用程序和系统漏洞暴露出来。当技术环境未得到及时修复时，攻击者就会利用漏洞发动攻击。

企业该如何实施此项控制措施？

虽然漏洞管理流程执行起来十分复杂，但大体上可以概括为五个步骤：[4]

1. **准备。**分析漏洞，确定资产范围，通知利益相关方和资产所有者，制定漏洞扫描计划。
2. **漏洞识别与检测。**这可以通过漏洞扫描实现。
3. **确定补救措施。**要精准确定补救措施，必须进行IT风险评估。视补救措施（例如补丁或配置更改）、软件限制和可用解决方案不同，可能会出现多种选择，包括：
   - 缓释，采取补救措施。
   - 接受，启动特例处理流程[5]并调查潜在攻击指标（IOC）。
4. **实施规定行动。**部署前述行动中识别的任务。
5. **监控漏洞。**新的漏洞不断出现，实时、持续监控对于妥善管理漏洞至关重要。

大多数漏洞都可以通过打补丁和更新系统来修复。对于存在已知漏洞且打补丁受限或者没有可用解决方案的系统，可检查是否存在攻击指标。如果此类系统遭到破坏，则应启动事件响应和恢复计划。此外，还可以为原有遗留系统制定隔离计划。最终，如果IT风险评估表明由于操作限制导致补救延迟，应执行特例处理流程。

保险公司也可能要求企业采取以下行动：

- 定期开展漏洞分析。
- 开展渗透测试。也就是说，至少每年进行网络攻击模拟演练，以检查可能被利用的漏洞。
- 信息技术和通讯环境的持续维护与更新。
- 自发布后三到七天内使用CVE[6] 8及以上补丁修复存在风险的IT系统。
- 非关键补丁，应于发布后30天内使用。

上述行动的频率和细节与企业的网络风险状况、所在行业及网络攻击环境有关。

3. 来源于 NIST SP 800-16. 然而，风险定义有很多种。虽然我们采用的是最简单的风险定义方式，但风险的最主要特征都涵盖在其中：发生可能性、威胁或事件、脆弱性以及影响。
4. SANS研究院的文章“Implementing a vulnerability management process.”对这些步骤进行了详细介绍。
5. 特例处理流程：与政策、标准和/或流程所述正常安全预期不一致的情况，例如，未应用补丁。
6. CVE代表常见漏洞和风险，是MITRE推出的一个程序，用于识别和分类软件或固件中的漏洞。

事件响应计划

这是一项怎样的控制措施？

事件响应计划记录了一套“预先设定的用于侦测、应对和控制针对企业IT系统所受恶意网络攻击的指令或流程”。[7]事件响应计划应与其他相关计划保持一致，包括：

- IT灾难恢复计划（DRP），该计划描述了企业在危机或灾难期间和之后应如何恢复数据。
- 业务连续性计划（BCP），其中阐述了企业应如何确保关键业务流程在危机或灾难期间和之后正常运行。

只有所有利益相关方都熟悉事件响应计划，它才能够顺利运行。因此，定期开展流程测试是该项控制措施中不可或缺的一部分。

企业为什么应采取此项控制措施？

事件响应计划对于提高企业网络复原力不可或缺。这些计划并非孤立的框架，它们应体现企业的特定风险状况，并被纳入到企业整体网络风险管理战略中。

对于缓释网络风险，技术和预防措施永远是首选方法和第一道防线。当网络事件发生时，尽早发现并进行快速专业的应对至关重要。

一份与时俱进的事件响应计划和一支训练有素的响应团队可以确保企业高效、快速并妥善的应对网络事件。当企业把事件响应计划与企业整体控制措施（12项主要控制措施）结合起来，并辅以适当的技术控制以及事件和灾难恢复（例如安全、加密和备份测试）努力，可显著降低网络事件对企业运营和安全的影响。

企业该如何实施此项控制措施？

我们建议企业在事件响应规划和测试中采取下列行动：

- 事件响应计划必须包含明确的网络事件处理、报告和恢复流程与程序。
- 明确事件响应团队成员在处理安全事件期间的角色、任务和责任。另外，必须确定上报路径和决策过程/职责。
- 规划和记录由外部承担的事件响应工作（例如IT取证调查）以及相关联系人信息。
- 由于勒索软件攻击事件激增及其可能带来重大损失，应制定一份专门针对勒索软件危机场景的应对策略。
- 只有事件响应团队成员熟悉各自角色和职责并清楚了解基本流程时，事件响应计划才能发挥应有的作用。企业应每年组织一次桌面演练，为事件响应团队提供特定场景培训，并评估企业对网络事件的应对准备情况。
- 另外，企业应定期审查和更新事件响应计划，将人员变动以及预期风险等新情况纳入考量范围内。

7. 请参见计算机安全资源中心Computer Security Resource Center的定义。

在企业遇到的网络安全问题中，
有95%都是由人为错误引发。[8]

网络安全意识培训及钓鱼攻击测试

这是一项怎样的控制措施？

网络安全意识培训是一种风险控制手段，旨在为员工和IT用户提供网络风险教育。该培训可帮助员工和IT用户识别各种攻击并掌握必要信息，通过预防攻击并在攻击或入侵企图发生之后采取正确措施，保护自己和公司。

网络钓鱼攻击测试是安全意识培训计划的一部分，通过模拟网络钓鱼攻击，向员工发送钓鱼邮件（虚假但非常逼真），测试其安全意识。网络钓鱼攻击测试通过评估员工对电子邮件的反应来验证员工安全意识培训的有效性，并确定改进所需行动。

企业为什么应采取此项控制措施？

企业是人员、流程和技术的组合。进行流程和技术投资很重要，但也不能忽略人为因素。全球95%的网络安全问题可以归因于人为错误。[8]

尽管企业拥有良好的IT安全性，但人为因素，如工作量、压力、缺乏技能、混合工作模式的增多以及基本的人性，都可能导致人为错误。然而，当安全链中最薄弱的环节得到合理关切时，它就可以变成最强有力的防御。

人为因素也是监管机构关注的问题之一。一些法规，包括但不限于支付卡行业数据安全标准（PCI-DSS）、美国国家标准和技术协会规章（NIST）、健康保险可携性和责任法案（HIPAA）以及通用数据保护条例（GDPR），可能要求员工定期接受安全意识培训。

网络安全意识培训和网络钓鱼攻击测试对于企业创建安全文化、将人为因素纳入网络安全计划、遵守法律法规并最终保护自己免受潜在网络事件的影响，十分重要。

企业该如何实施此项控制措施？

企业在建立网络安全意识时应采取下列行动：

1. 每年进行一次分析，查找网络安全技能缺口，并制定和实施培训路线图和/或项目计划，以弥合缺口。
2. 创建年度（至少）网络安全意识培训计划：
   - 对所有员工、供应商/承包商和第三方合作伙伴具有强制性。
   - 训练用户规避常见的网络风险和威胁，例如社交工程和网络钓鱼攻击。
   - 定期（至少每年一次）更新内容，纳入新型攻击和社交工程攻击应对技术。
3. 至少每年开展一次内部网络钓鱼攻击演练活动。
4. 制定流程，用于向内部安全团队报告可疑电子邮件，以便其开展调查。
5. 制定网络钓鱼攻击应对流程。
6. 标记外部邮件，提醒员工该邮件来自公司外部。

美国国家标准和技术协会（NIST）也在其网络框架“保护职能”项下阐述了网络安全意识培训的重要性。如需进一步指导，请参阅：“NIST Special Publication 800-50.”

8. Mee, P. and Brandenburg, R. 2020: “After reading, writing, and arithmetic, the fourth ‘r’ of literacy is cyber-risk.” 世界经济论坛全球议程，2020年12月17日。

9

远程桌面协议风险缓释及其它强化技术

这是一项怎样的控制措施？

强化是将安全配置应用于系统（包括服务器、应用程序、操作系统、数据库、安全和网络设备）以符合最佳实践的过程。安全配置是指通过限制内部网络各个平台或互联网的风险，从而降低企业的网络攻击成本。

企业为什么应采取此项控制措施？

通过强化技术，企业可阻止未使用或不安全的设备、缓释漏洞并改善可能被恶意攻击者利用的薄弱配置，从而最大程度减少攻击面。

企业该如何实施此项控制措施？

通常，企业会按照最佳实践为其主要系统和服务确立一组安全配置，即安全基准或强化指南。企业还会实施相关流程，用于部署这些配置并开展定期检查，以识别错误配置或偏差。

虽然不同平台的配置存在差异，但安全基准一般都包含下列配置：

- 用户和访问管理。
- 密码政策。
- 安全服务和协议。
- 防火墙配置。
- 网络配置。
- 远程访问。
- 日志管理和审查政策。
- 病毒/恶意软件防护。
- 应用程序控制。
- 安全更新。
- 加密。
- 其他平台特定的安全配置。

为了确保及时部署这些配置，企业可以使用在运行安全配置或工具的系统映像，然后定期开展缺口分析。

那些薄弱或经常遭受攻击的协议或服务，例如远程桌面协议（RDP）、服务器信息拦截（SMB）、安全外壳（SSH）、文件传输协议（FTP）以及数据库端口，是保险公司关注的一个重点。企业需要执行严格的强化流程，以消除这些端口在互联网上的使用。如果出于特定业务需求，确实需要使用这些端口，企业则应实施额外控制措施，以降低相关风险。

企业在实施强化流程时可能遇到的一个常见障碍就是缺乏全面的资产清单，无法为企业提供详细的网络技术信息（这些信息可为关键流程提供支持）。

我们建议企业创建结构化变革管理流程，以部署安全基准。如果没有适当的流程，部署时所需的配置可能失效，从而影响系统的可用性。企业可能需要进行更加深入的分析，以找到一种安全的方法来运行应用程序或者要求对应用程序做出变更。如今，供应商和网络安全组织不断发布针对最常用系统和服务的安全基准。互联网安全中心（CIS）是最主要的安全基准发布组织，所有企业均可访问获取。

日志记录与监控

这是一项怎样的控制措施？

为了及时应对网络攻击，企业需要具备强大的日志记录与监控能力，以识别网络上的任何可疑活动。要做到这一点，企业需掌握特定知识并拥有适当的工具和流程。所有这些工作通常都是由安全运营中心（SOC）或外部管理的安全服务供应商（MSSP）负责完成。SOC或MSSP可能提供不同的服务，具体取决于他们的成熟度。

企业为什么应采取此项控制措施？

鉴于当前的全球风险形势，企业不仅需要实施一系列预防网络攻击的控制措施，还需要识别任何可能导致网络攻击以及触发网络事件响应计划的可疑活动。要做到这一点，企业必须依靠其主系统或应用程序中的日志记录配置、事件收集、关联和预警工具以及在事件发生后能够开展分析和采取行动的团队。

企业该如何实施此项控制措施？

我们建议企业：

1. 执行审计日志功能，确定需要监控的系统或平台，包括防火墙、入侵预防和检测系统、活动目录、防病毒/防恶意软件、端点安全技术（例如端点检测与响应EDR和延伸检测与响应XDR）、数据丢失预防（DLP）、应用程序、Microsoft 365以及企业确定的其他重要平台。
2. 部署安全事件管理系统（SIEM）并将主要平台纳入该系统中。应至少保留三个月的日志记录和一年期日志记录备份。
3. 分析网络中的日志记录，并确定一组企业希望进行监控和响应的使用场景或常见模式。这些信息还应与风险情报信息联合使用。
4. 确定相关流程，用于定期审查关键系统中管理员或高权限用户的活动。
5. 建立并培训一支专业团队，专门监控安全事件及响应情况。
   - 制定专门的流程或手册，以便在侦测到网络安全事件时SOC及MSSP可以做出反应。如果这项服务被外包，上述流程还应涵盖企业为控制和消除网络安全风险以及恢复运营所需执行的任务。
   - 确定并监控关键绩效指标，以便持续改进。

要具备强大的日志记录和监控能力，企业不仅需要投入大量资金和资源，还需要进行持续审查，以确保相关流程能够检测到现实中的可疑活动。

寿命终止系统的更换与保护

这是一项怎样的控制措施？

寿命终止（EOL）或支持终止（EOS）产品是指寿命到达终点的产品。对于此类产品，供应商不再提供补丁和其它形式的安全支持，用户无法获取更新，因而会带来风险。没有技术支持，产品漏洞将无法得到修复。

要缓释这一风险，唯一的办法就是停止使用过时的产品，用更新的解决方案进行替代或升级，以继续提供支持。如果做不到这一点，企业需要采取额外控制措施来保护EOL/EOS系统，例如限制对这些系统的访问，确保它们不暴露在互联网环境中，并与其他物体隔离。

企业通常会将EOL/EOS产品和系统用于大型遗留系统中，尤其是使用这些系统进行运营技术（OT）控制，在这种情况下系统定期升级很难实现且成本高昂。

企业为什么应采取此项控制措施？

EOL/EOS产品中的漏洞处于未修复状态，因此被越来越多的、寻求简单方式入侵系统的黑客所利用。由于论坛会公开讨论已知漏洞，黑客可以轻松发现仍在使用中的EOL系统。

虽然开放端口和电子邮件钓鱼攻击仍然是主流攻击手段，但已知的软件漏洞也是一个常见的切入点，为进入系统提供了一条简单的途径。一旦进入，黑客会试图通过网络获取访问权限，窃取有价值的数据并对系统实施加密。

企业该如何实施此项控制措施？

理想的做法是，企业停止使用任何过时的产品。如果这行不通，企业应确保遗留系统得到保护。限制从外部访问这些产品是关键的一步，如果攻击者无法进入设备，则设备被利用的风险会大大降低。如果可能的话，企业应采取网络隔离措施。如果不行，则企业应部署独立的网络防火墙并监控流向过时服务器的数据流。将所有来自互联网的访问设为不可信，是一种值得借鉴的做法。

企业还可以采取措施来控制网络攻击的潜在影响，例如禁用EOL系统访问或存储关键和敏感数据或系统，做到这一点，即使EOL设备受到攻击，后果也不会特别严重。

升级EOL系统和产品可能产生高昂的成本。对于拥有大量遗留设备和操作技术系统的企业，EOL产品可能意味着整个系统大修或升级换代。

如果企业选择继续使用EOL产品，则应采取必要的风险防护和缓释措施。这不仅需要IT和OT安全团队携手合作，还需要外部专业知识和工具的支持。对于拥有大量OT系统的制造商和其他企业，实施起来可能会非常复杂和耗时。

数字化供应链的网络风险管理

这是一项怎样的控制措施？

数字化供应链涵盖所有信息技术（IT）和运营服务（OT）供应商，他们与企业团队联合提供数字化服务。在网络风险方面，数字化供应链带来了日益严峻的挑战。事实上，许多大型数字化供应链漏洞都造成了重大影响，例如，最近的Log4J和Kaseya漏洞以及黑客入侵事件（例如云料斗行动Operation Cloud Hopper）。就连臭名昭著的NotPetya攻击也是源自数字化供应链风险。

数字化供应商提供了一个可以访问数百家公司及其敏感数据的完美切入点。网络犯罪分子只要突破一家数字化供应商的漏洞，就可以进入其客户的网络和设备。

企业亟需一个稳健的框架，以管理其数字化供应链的网络风险。

企业为什么应采取此项控制措施？

随着数字化程度的不断提高，企业越来越多的使用信息和通信技术来交付关键产品和服务，这也带来了新的网络风险，企业需要加以妥善管理。另一方面，企业也在使用不同供应商提供的新型差异化数字服务，通过软件包获取外包和软件即服务[9]产品。与此同时，供应链的日益全球化在保密性、完整性和可用性方面带来了新的风险。

随着数字化服务的普及，数字化供应链管理变得越来越复杂。由于“影子IT[10]”问题，IT团队可能并不了解企业使用的全部服务，因而服务中包含哪些构成环节以及存在哪些潜在漏洞也不是显而易见的。网络罪犯分子经常使用数字化供应链作为一种网络攻击机制。事实上，大多数软件产品依赖供应商提供的成千上万的预写包。常用第三方软件供应链中的构成环节是网络犯罪分子特别喜欢的攻击目标，因为他们只要攻入一家数字化服务供应商的网络，即可获得该供应商多家客户的访问权限。

因此，该项控制措施旨在通过采取一系列措施，分析、管理和应对网络风险，从而保护数字化供应商免受网络风险影响。

企业该如何实施此项控制措施？

我们建议企业采取下列措施管理数字化供应链风险：

- 采用数字化供应链风险管理框架，包括基于高水平风险量化的一级供应商风险评级。这有助于企业进行风险管理和资本分配战略决策。
- 实施网络安全框架，包括但不限于：
  - 基于“零信任”预期和“需要知晓”原则管理账户。特权账户和普通账户严格适用。
  - 执行基于风险的多重身份验证。
  - 与内部安全运营中心合作，设定具体使用场景，监控第三方访问。
- 制定针对供应商/数字化供应链场景的事件响应手册并开展测试演练，将第三方纳入其中。
- 评估各家数字化供应商的合同、服务协议和上报协议。
- 与采购部门合作，在新签和续签合同时纳入网络安全卫生相关控制和责任要求，可包含安全培训和认证。

9. 软件即服务（Software-as-a-service，SaaS）是一种软件分发模型，云服务供应商在其中托管应用程序并通过互联网提供给终端用户。
10. 影子IT指在IT或信息安全部门之外实施的信息技术计划、项目或系统。

利用达信推荐的控制措施，进一步强化网络安全与复原力

达信认为，在新的网络风险模式下，企业应接受现代商业已进入数字化经营这一事实，并采取新的方法，持续了解、衡量和管理网络风险。新型网络风险层出不穷，通过严格的训练，企业将进一步提升前瞻和灵活转变能力，从而取得更好的结果。

通过实施我们推荐的控制措施，企业可以预防并应对大多数网络攻击，最大程度降低网络攻击的影响。企业将做好自我防护准备，并从容构建网络复原能力。鉴于当前的网络环境以及企业面临的日趋严峻的风险，网络复原力不再是事后诸葛亮或打勾的练习，它已成为最起码的要求。

了解更多信息

关于网络复原力的第一手资料是非常宝贵的。达信拥有超过25年网络风险服务经验以及丰富的数据驱动型见解，深入了解全球企业面临的网络风险威胁。我们始终站在行业前沿，可以帮助您弥合风险、保险和网络安全之间的缺口，将网络风险与企业风险关联起来，并做出审慎的资本投资决策。

我们与客户携手合作，提高企业网络风险治理水平，推动各主要利益相关方切实行动起来以妥善应对网络风险这一重要问题，并为企业管理层和董事会决策提供支持。

达信拥有专门的网络风险咨询顾问团队，可以兼顾保险和网络安全两个领域，为您提供适用于整个企业层面、经过量化的网络风险观，并协助您完成网络风险复原规划。我们提供量身定制的网络风险保险和咨询解决方案，帮助您管理网络风险并带来高效的风险转移选项。

欲知更多关于贵公司如何更好地理解、衡量和管理网络风险的信息，请联系达信专员或者点击此处联系我们。

关于达信

达信（Marsh）是全球领先的保险经纪和风险咨询公司，在130多个国家大约有45,000名员工，致力于向全球商业企业和个人客户提供数据驱动型风险解决方案和咨询建议服务。达信是Marsh McLennan（纽交所代码：MMC）的旗下公司，后者是一家全球性专业服务公司，向客户提供风险、战略和人力资源服务，年收入超过200亿美元，通过旗下四家处于市场领先地位的子公司帮助客户在变化多端和日趋复杂的环境中不断发展壮大。除达信以外，Marsh McLennan还是佳达、美世和奥纬的母公司。了解更多信息，请访问mmc.com，或者在微信公众号搜索MarshChina关注达信微信公众平台，或者订阅BRINK获取相关信息。